## REMARKS

Claims 1-33 are presented for examination. Claims 1, 6, 10, 20, 25, and 30-33 have been amended to define more clearly what Applicants regard as their invention. Claims 1, 10, 20, 25, and 30-33 are in independent form. Favorable reconsideration is requested.

Claims 32 and 33 were rejected under 35 U.S.C. § 101 as allegedly being directed to non-statutory subject matter for claiming a computer program. Without conceding the propriety of this rejection, Claims 32 and 33 have been amended to recite a program product stored on a computer-readable storage medium, the program product embodying a software program, which constitutes statutory subject matter under MPEP § 2106(IV)(B)(1)(a). Accordingly, it is respectfully requested that the rejection of Claims 32 and 33 under Section 101 be withdrawn.

Claims 1-3, 6-8, 10-14, 16, 17, 20, 21, 25, and 27 were rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent 5,341,425 to Wasilewski et al. Claims 4, 5, 9, 15, 18, 19, 22-24, and 28-33 were rejected under 35 U.S.C. § 103(a) as being obvious from Wasilewski in view of U.S. Patent 5,319,705 to Halter et al.

Claim 1 is directed to a data processing apparatus including reception means, first encryption means, generating means, multiplexing means, and transmitting means. The reception means receives a plurality of transmitting requests of object data, and the first encryption means encrypts at least a predetermined portion of the object data using first key data to produce encrypted object data. The generating means generates seed information which allows the first key data to be obtained therefrom, the seed information

being generated after the reception means receives the transmitting requests. The multiplexing means multiplexes the plurality of object data and the encrypted object data to generate a data stream. The transmitting means individually transmits the seed information and the data stream, the seed information being transmitted after the reception means receives the transmitting requests.

Notably, in Claim 1, the transmitting requests are received and then the encrypted object data and the seed information, which allows the first key data used to produce the encrypted object data to be obtained therefrom, are individually transmitted. By virtue of the features of Claim 1, it can be easier to assure security rather than transmitting a key itself which is used for encryption, or transmitting a key and seed information together with encrypted data.

Furthermore, by virtue of the features of Claim 1, security can be kept at a reproducing side without the necessity to safely keep the seed information, since the seed information is generated to be transmitted after receiving the transmitting requests.

Wasilewski et al., as understood by Applicants, relates to encrypting data at a plurality of data transmission sites for transmission to a reception site. A set of data is encrypted at each of a plurality N of transmission sites for transmission to and subsequent decryption at at least one reception site. Each of the N transmission sites is provided with a broadcast key unique to that transmission site and a system key that is the same for all transmission sites. The system key comprises a plurality S of bits and each of the N broadcast keys comprises a unique plurality B of bits, wherein B is less than S. At each transmission site, the system key and the broadcast key unique to that transmission site are

convolved in a predetermined manner to generate a unique data encryption key for that transmission site. The unique encryption key generated at each transmission site comprises a third number E of bits, E being at least greater than B. Preferably, E is greater than or equal to S. At each transmission site, a set of data is then encrypted with the unique data encryption key generated at that site. The sets of data uniquely encrypted at each transmission site are then transmitted to the reception site. There is stored, in a memory at the reception site, the system key and each of the broadcast keys to enable a selected one of the encrypted sets of data to be decrypted at the reception site. (See column 3, cited in the Office Action, and Figs. 2-5.)

At pages 2 and 3 of the Office Action, the Examiner states that Wasilewski et al. teaches "seed information (pk program key, system key/ Sk, broadcast key/ Bk, col. 3, lines 12 et seq)..."

However, the system key and broadcast key of Wasilewski et al. are previously kept on both the transmitting side and the reception side, and are not what is generated. That is, the system key and broadcast key of Wasilewski et al. are required to be safely kept at the reproducing side all the time and, consequently, with the system of Wasilewski et al. it is difficult to keep security.

On the contrary, in Claim 1, the transmitting requests are received and then the encrypted object data and the seed information, which allows the first key data used to produce the encrypted object data to be obtained therefrom, are individually transmitted. Moreover, in Claim 1, the seed information is generated to be transmitted after receiving the transmitting requests.

As to the program key of Wasilewski et al. (see Fig. 3 of that patent), the program key is multiplexed with the encrypted program data and is transmitted. Thus, the system of Wasilewski et al., in which a key is transmitted together with the encrypted data, cannot assure security.

Nothing has been found in Wasilewski that would teach or suggest that (1) transmitting requests are received and then encrypted object data and seed information, which allows first key data used to produce the encrypted object data to be obtained therefrom, are individually transmitted, and (2) the seed information is generated to be transmitted after receiving the transmitting requests, as recited in Claim 1.

Accordingly, Claim 1 is seen to be clearly allowable over Wasilewski et al.

Independent Claims 10, 20, and 25 recite features similar in many respects to those discussed above with respect to Claim 1 and therefore are also believed to be patentable over Wasilewski et al. for at least the reasons discussed above.

Independent Claims 30-33 also recite features similar in many respects to those discussed above with respect to Claim 1. Moreover, nothing has been found in Halter et al. that would remedy the deficiencies of Wasilewski et al., discussed above in connection with Claim 1. Accordingly, Claims 30-33 are believed to be patentable over Wasilewski et al. and Halter et al., whether considered either separately or in any permissible combination (if any).

A review of the other art of record has failed to reveal anything which, in Applicants' opinion, would remedy the deficiencies of the art discussed above, as

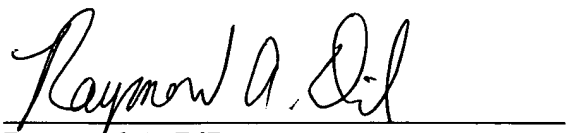
references against the independent claims herein. Those claims are therefore believed patentable over the art of record.

The other claims in this application are each dependent from one or another of the independent claims discussed above and are therefore believed patentable for the same reasons. Since each dependent claim is also deemed to define an additional aspect of the invention, however, the individual reconsideration of the patentability of each on its own merits is respectfully requested.

In view of the foregoing amendments and remarks, Applicants respectfully request favorable reconsideration and early passage to issue of the present application.

Applicants' undersigned attorney may be reached in our New York office by telephone at (212) 218-2100. All correspondence should continue to be directed to our below listed address.

Respectfully submitted,



Raymond A. DiPerna
Attorney for Applicants
Registration No.: 44,063

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200